UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,619	08/30/2000	Richard H. Boive	YOR9-0351	1129

7590 06/28/2005

Harry F Smith Esq
Ohlandt Greeley Ruggiero & Perle L L P
One Landmark Square
Suite 903
Stamford, CT 06901

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/651,619	**Applicant(s)** BOIVE, RICHARD H.	
	Examiner Aravind K. Moorthy	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 28 April 2005.

2. Claims 1-22 are pending in the application.

3. Claims 1-22 have been rejected.

Response to Arguments

4. Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 2, 5, 9, 10, 12, 16-19 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Yavatkar et al U.S. Patent No. 6,735,702 B1.

As to claim 1, Yavatkar et al discloses a method for tracing a denial-of-service attack on a victim machine back towards its source, comprising steps of:

> operating a traceback program on at least one path to receive two input parameters, (a) an IP address (v) of the victim machine and (b) an IP address (r) of a router that is immediately upstream of the victim machine [column 13, lines 30-43];

determining a set of routers that are neighbors (n) of r [column 16 line 66 to column 17 line 31];

for each neighbor n of r, determining if r is n's next-hop for traffic addressed to v, or to a network that v is on, where node n's next-hop for traffic addressed to v is the IP address of the node that n will forward a packet to if the destination address in the packet is v [column 17, lines 32-51].

if r is not n's next-hop for traffic addressed to v, skip over n and query the next neighbor of r, while if r is n's next-hop for traffic addressed to v, determining an amount of traffic that n is forwarding to r that is addressed to v [column 17, lines 32-51].

after determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v, continuing one node further upstream from the determined neighbor n of r that is the principal source of packets flowing to r that are addressed to v, and continuing to traceback through interconnected routers until a source of denial-of-service attack packets to v is determined or until further traceback is not possible [column 17, lines 52-67].

As to claims 2 and 10, Yavatkar et al discloses that the step of determining the set of neighbors comprises a step of sending at least one query to r to obtain information from a MIB that stores IP addresses of routers that are neighbors of r [column 15, lines 42-62].

As to claims 5 and 12, Yavatkar et al discloses that the step of determining an amount of traffic comprises a step of sending at least one message to a neighbor router n for determining a count of packets that router n is sending to router r that are addressed to v or to a network on which v resides [column 15, lines 42-62].

As to claim 9, Yavatkar et al discloses a backtracking unit for tracing a denial-of-service-attack on a victim machine back towards its source, comprising a computer-readable media for receiving a first input parameter of an IP address (v) of the victim machine and a second input parameter of an IP address (r) of a router that is immediately upstream of the victim machine [column 13, lines 30-43], the trackback computer program controlling operation of the data processor to determine a set of routers that are neighbors (n) of r [column 16 line 66 to column 17 line 31], for each neighbor n of r, determining if r is n's next-hop for traffic addressed to v, where node n's next-hop for traffic addressed to v is the IP address of the node that n will forward a packet to if the destination address in the packet is v, the traceback computer program further controlling operation of the data processor for the case where r is not n's next-hop for traffic addressed to v, to skip over n and to query the next neighbor of r, while for the case where r is n's next-hop for traffic addressed to v, to determine an amount of traffic that n is forwarding to r that is addressed to v [column 17, lines 32-51], and after determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v or to a network to which v is connected, for continuing one node further upstream from the determined neighbor n of r that is the principal source of packets flowing to r that are addressed to v to continue to traceback through interconnected routers until a source of denial-of-service attack packets to v is determined or until further traceback is not possible [column 17, lines 52-67].

As to claim 16, Yavatkar et al discloses a method for determining an identity of a source of undesirable packets received from a data communications network, comprising steps of:

operating a traceback program on at least one path to receive two input parameters, (a) an IP address (v) of the victim machine and (b) an IP address (r) of a router that is immediately upstream of the victim machine [column 13, lines 30-43];

determining a set of routers that are neighbors (n) of r [column 16 line 66 to column 17 line 31];

for each neighbor n of r, determining if r is n's next-hop for traffic addressed to v, or to a network that v is on, where node n's next-hop for traffic addressed to v is the IP address of the node that n will forward a packet to if the destination address in the packet is v [column 17, lines 32-51].

if r is not n's next-hop for traffic addressed to v, skip over n and query the next neighbor of r, while if r is n's next-hop for traffic addressed to v, determining an amount of traffic that n is forwarding to r that is addressed to v [column 17, lines 32-51].

after determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v, continuing one node further upstream from the determined neighbor n of r that is the principal source of packets flowing to r that are addressed to v, and continuing to traceback through interconnected routers until a source of denial-of-service attack packets to v is determined or until further traceback is not possible [column 17, lines 52-67].

As to claim 17, Yavatkar et al discloses that the steps of determining and querying each comprise a step of sending queries to the data communications network [column 16, lines 22-45].

As to claim 18, Yavatkar et al discloses that the step of querying comprises steps of: sending a first network message to a packet router for instructing the packet router to determine a number of packets that it is sending addressed to v [column 16, lines 22-45]. Yavatkar et al discloses sending a second network message to the packet router to query the packet router for the determined number [column 16, lines 22-45].

As to claim 19, Yavatkar et al discloses that the step of querying comprises a step of sending at least one message to a packet router for determining a number of packets being forwarded to or towards v [column 16, lines 22-45].

As to claim 21, Yavatkar et al discloses that the step of operating the traceback function operates the traceback function on a plurality of selected paths. Yavatkar et al discloses that a particular path is selected based at least on an amount of traffic flowing through the path traceback through interconnected routers until a source of denial-of-service attack packets to v is determined, or until further traceback is not possible [column 16, lines 50-65].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 3, 4 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al U.S. Patent No. 6,735,702 B1 as applied to claims 1 and 9 above, and further in view of Li et al U.S. Patent No. 6,535,507 B1.

As to claims 3, 4 and 11, Yavatkar et al does not teach that the step of determining if r is n's next-hop for traffic addressed to v comprises a step of sending at least one query to router n. Yavatkar et al does not teach that the step of sending at least one query queries an IP Forwarding Table MIB of router n.

Li et al teaches determining if r is n's next-hop for traffic addressed to v comprises a step of sending at least one query. Li et al teaches sending at least one query queries an IP Forwarding Table [column 6, lines 46-54].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al so that if it was determined that if r was n's next-hop for traffic addressed to v then a query would have been sent to router n. The query would have been an IP Forwarding Table of router n.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al, as described above, by the teaching of Li et al because it provides automated maintenance of translation tables which may be tailored to meet the operating policy of network managers that control respective domains [abstract].

7. **Claims 6 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al U.S. Patent No. 6,735,702 B1 as applied to claims 1 and 9 above, and further in view of Bhaskaran U.S. Patent No. 5,963,540.**

As to claims 6 and 13, Yavatkar et al does not teach a step of establishing a black hole host route to v as close as is possible to the source of the denial-of-service attack packets.

Bhaskaran teaches establishing a black hole host route to v as close as is possible to the source of the attack [column 1, lines 53-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al so that there would have been a black hole host route as close as possible to the source of the attack.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al, as described above, by the teaching of Bhaskaran because it helps reduce the amount of denial of service attack packets in the network [column 1, lines 25-39].

8. Claims 7 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al U.S. Patent No. 6,735,702 B1 as applied to claims 1 and 9 above, and further in view of Hughes U.S. Patent No. 6,636,509 B1.

As to claims 7 and 14, Yavatkar et al does not teach a step of establishing a special host route to v using the same next hop as an existing route. Yavatkar et al does not teach that the special host route tracking changes in the existing route such that when a next hop for the existing route changes, the next hop for the host route changes similarly.

Hughes teaches establishing a special host route to v using the same next hop as an existing route. Yavatkar et al does not teach that the special host route tracks changes in the existing route such that when a next hop for the existing route changes, the next hop for the host route changes similarly [column 6, lines 11-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al so that there would have been a special route using the same next hop as an existing route. The special host route would have tracked changes in the existing routes so that when a next hop for the exiting route changed, the next hop for the host route would have changed similarly.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al, as described above, by the teaching of Hughes because by using special routes it reduces the amount of hops in the routing table [column 3, lines 6-29]

9. Claims 8 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al U.S. Patent No. 6,735,702 B1 as applied to claims 1 and 9 above, and further in view of Packer U.S. Patent No. 6,298,041 B1.

As to claims 8 and 15, Yavatkar et al does not teach a step of establishing a rate limit for packets addressed to v as close as is possible to the source of the denial-of-service attack packets.

Packer teaches establishing a rate limit for packets addressed [column 4 line 50 to column 5 line 7].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al so that there would have been a rate limit for packets addressed to v as close as is possible to the source of the denial-of-service attack packets.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al, as described above, by the teaching of Packer because rate control is introduced into a level of a packet communication environment at which there is a lack of data rate supervision to control assignment of available bandwidth from a single logical link to network flows [column 3, lines 22-32].

10. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al U.S. Patent No. 6,735,702 B1 as applied to claim 16 above, and further in view of Bare U.S. Patent No. 6,456,597 B1.

As to claim 20, Yavatkar et al does not teach establishing at least one of a black hole host route to v as close as is possible to the source of the undesirable packets. Yavatkar et al does not teach establishing a special host route to v using the same next hop as an existing route, the special host route tracking changes in the existing route such that when a next hop for the existing route changes, the next hop for the host route changes similarly. Yavatkar et al does not teach establishing a rate-limit for packets addressed to v as close as is possible to the source of the denial-of-service attack packets.

Bare teaches establishing at least one of a black hole host route to v as close as is possible to the source of the undesirable packets [column 41 line 66 to column 42 line 45. Bare teaches establishing a special host route to v using the same next hop as an existing route, the special host route tracking changes in the existing route such that when a next hop for the existing route changes, the next hop for the host route changes similarly [column 38 line 33 to column 39 line 13]. Bare teaches establishing a rate-limit for packets addressed to v as close as is possible to the source of the denial-of-service attack packets [column 77, lines 51-60].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al, as described above, so that a black hole host route would have been established as close as is possible to the source of the undesirable packets. A special host route using the same next hop as an existing route would have been established, the special host route tracking changes in the existing route such that when a next hop for the existing route changes, the next hop for the host route changes similarly. There would have been a rate-limit for packets addressed to v as close as is possible to the source of the denial-of-service attack packets.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al by the teaching of Packer because using any of the above methods, you reroute any undesired packets away from the network.

11. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al U.S. Patent No. 6,735,702 B1 in view of Bhaskaran U.S. Patent No. 5,963,540.

As to claim 22, Yavatkar et al discloses a method for tracing a denial-of-service attack on a victim machine back towards its source, comprising steps of:

> operating a traceback program on at least one path to receive two input parameters, (a) an IP address (v) of the victim machine and (b) an IP address (r) of a router that is immediately upstream of the victim machine [column 13, lines 30-43];
>
> determining a set of routers that are neighbors (n) of r [column 16 line 66 to column 17 line 31];
>
> for each neighbor n of r, determining if r is n's next-hop for traffic addressed to v, or to a network that v is on, where node n's next-hop for traffic addressed to v is the IP address of the node that n will forward a packet to if the destination address in the packet is v [column 17, lines 32-51];
>
> if r is not n's next-hop for traffic addressed to v, skip over n and query the next neighbor of r, while if r is n's next-hop for traffic addressed to v, determining

an amount of traffic that n is forwarding to r that is addressed to v by sending at least one message to a neighbor router n for determining a count of packets that router n is sending to router r that are addressed to v or to a network on which v resides [column 17, lines 32-51];

after determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v, continuing one node further upstream from the determined neighbor n of r that is the principal source of packets flowing to r that are addressed to v, and continuing to traceback through interconnected routers until a source of denial-of-service attack packets to v is determined or until further traceback is not possible [column 17, lines 52-67]; and

Yavatkar et al does not teach a step of establishing a black hole host route to v as close as is possible to the source of the denial-of-service attack packets.

Bhaskaran teaches establishing a black hole host route to v as close as is possible to the source of the attack [column 1, lines 53-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al so that there would have been a black hole host route as close as possible to the source of the attack.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yavatkar et al, as described above, by the teaching of Bhaskaran because it helps reduce the amount of denial of service attack packets in the network [column 1, lines 25-39].

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
June 24, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100